

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF OKLAHOMA

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. CR-21-358-RAW

SILVIA VERONICA FUENTES,

Defendant.

**UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS
EVIDENCE OBTAINED BY GOOGLE "GEOFENCE" SEARCH WARRANT
AND BRIEF IN SUPPORT**

Respectfully submitted,

CHRISTOPHER J. WILSON
United States Attorney

/s/ T. Cameron McEwen
T. CAMERON MCEWEN
AL BAR # 7161-R67M
Assistant United States Attorney
Eastern District of Oklahoma
520 Denison Ave.
Muskogee, OK 74401
(918) 684-5100
Cameron.McEwen@usdoj.gov

November 30, 2022

TABLE OF CONTENTS

UNITED STATES’ RESPONSE TO DEFENDANT’S MOTION TO SUPPRESS EVIDENCE OBTAINED BY GOOGLE “GEOFENCE” SEARCH WARRANT AND BRIEF IN SUPPORT	1
I. BACKGROUND.....	1
II. ARGUMENT.....	8
<i>A. Defendant Had No Reasonable Expectation of Privacy in the Four Minutes of Google Location Information</i>	<i>8</i>
1. <i>Obtaining Four Minutes of Defendant’s Location Information Was Not a Search Under Carpenter</i>	<i>9</i>
2. <i>Defendant Has No Reasonable Expectation of Privacy in Location Information She Disclosed to Google.....</i>	<i>14</i>
<i>B. The Geofence Warrant Satisfied the Fourth Amendment.....</i>	<i>17</i>
1. <i>The Geofence Affidavit Established Probable Cause.....</i>	<i>18</i>
2. <i>The Geofence Warrant Specified its Objects with Particularity.....</i>	<i>23</i>
<i>C. Evidence from the Geofence Warrant Should Not be Suppressed Because Investigators Relied Upon It in Good Faith.....</i>	<i>27</i>
CONCLUSION.....	31
Exhibit 1	<i>Google Geofence Search Warrant Application</i>
Exhibit 2	<i>Google Geofence Search Warrant</i>
Exhibit 3	<i>Google Account Number Search Warrant Application</i>
Exhibit 4	<i>Google Account Number Search Warrant</i>

TABLE OF AUTHORITIES

Federal Cases

<i>Alderman v. United States</i> , 394 U.S. 165 (1969)	23
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976).....	24
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018)	<i>passim</i>
<i>Dalia v. U.S.</i> , 441 U.S. 238 (1979)	23
<i>Davis v. United States</i> , 564 U.S. 229 (2011).....	24, 27
<i>District of Columbia v. Wesby</i> , 138 S. Ct. 577 (2018)	18
<i>Herring v. United States</i> , 555 U.S. 135 (2009)	27
<i>Hoffa v. United States</i> , 385 U.S. 293 (1966)	14
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983) (unpublished)	18
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	17
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987)	24
<i>Messerschmidt v. Millender</i> , 565 U.S. 535 (2012)	21, 29
<i>Mink v. Knox</i> , 613 F.3d 995 (10 Cir. 2010)	23
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978)	23

<i>SEC v. Jerry T. O’Brien, Inc.</i> , 467 U.S. 735 (1984)	14
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	12, 15, 6, 17
<i>States v. Miller</i> , 425 U.S. 435 (1976)	12, 14, 16, 17
<i>Steagald v. United States</i> , 451 U.S. 204 (1981)	17
<i>United States v. Adkinson</i> , 916 F.3d 605 (7th Cir. 2019)	10
<i>United States v. Anzalone</i> , 208 F. Supp. 3d 358 (D. Mass. 2016).....	26
<i>United States v. Artez</i> , 389 F.3d 1106 (10 Cir. 2004)	18
<i>United States v. Bosyk</i> , 933 F.3d 319 (4th Cir. 2019)	18
<i>United States v. Bynum</i> , 604 F.3d 161 (4th Cir. 2010)	8
<i>United States v. Chatrie</i> , 590 F.Supp.3d 901 (E.D. Virginia, Richmond Division 2022)	29-30
<i>United States v. Cookson</i> , 922 F.3d 1079 (10th Cir. 2019)	26
<i>United States v. Davis</i> , 542 F.2d 743 (8th Cir. 1976)	24, 27
<i>United States v. Hammond</i> , — F.3d —, 2021 WL 1608789 (7th Cir. Apr. 26, 2021).	10
<i>United States v. Hodge</i> , 354 F.3d 305 (4th Cir. 2004)	18

<i>United States v. Hurwitz</i> , 459 F.3d 463 (4th Cir. 2006).	23, 25
<i>United States v. James</i> , No. 18-cr-216, 2019 WL 325231 (D. Minn. Jan. 25, 2019)	21, 24, 25
<i>United States v. Kimble</i> , 855 F.3d 604 (4th Cir. 2017)	23
<i>United States v. Leon</i> , 468 U.S. 897 (1984)	27, 28, 29, 30
<i>United States v. Matish</i> , 193 F. Supp. 3d 585 (E.D. Va. 2016)	26
<i>United States v. Matthews</i> , 12 F.4th 647 (7th Cir. 2021).	30
<i>United States v. McLamb</i> , 880 F.3d 685, 688 (4th Cir. 2018)	27, 28, 30
<i>United States v. Otero</i> , 563 F.3d 1127 (10 Cir. 2009)	24
<i>United States v. Patrick</i> , 842 F.3d 540 (7th Cir. 2016)	23
<i>United States v. Perez</i> , 393 F.3d 457 (4th Cir. 2004)	28
<i>United States v. Perrine</i> , 518 F.3d 1196 (10th Cir. 2008)	8, 18
<i>United States v. Pulliam</i> , 748 F.3d 967 (10th Cir. 2014)	23
<i>United States v. Reed</i> , 195 Fed.Appx. 815 (10th Cir. 2006)	18
<i>United States v. Rhodes</i> , 2021 WL 1541050 (N.D. Ga. Apr. 20, 2021)	10

<i>United States v. Seerden</i> , 916 F.3d 360 (4th Cir. 2019)	29
<i>United States v. Taylor</i> , 935 F.3d 1279 (11th Cir. 2019)	26
<i>United States v. Torch</i> , 609 F.2d 1088 (4th Cir. 1979)	24
<i>United States v. Wagner</i> , 951 F. 3d 1232 (10th Cir. 2020)	26
<i>United States v. Walker</i> , 2020 WL 4065980 (W.D.N.C. July 20, 2020)	10
<i>United States v. Wellbeloved-Stone</i> , 777 F. App’x 605, 607 (4th Cir. June 13, 2019) (unpublished)	13
<i>United States v. Williams</i> , 592 F.3d 511 (4th Cir. 2010)	24
<i>United States v. Workman</i> , 863 F.3d 1313 (10th Cir. 2017)	26
<i>United States v. Yang</i> , 958 F.3d 851 (9th Cir. 2020) (concurrence)	11
<i>Voss v. Bergsgaard</i> , 774 F.2d 402 (10th Cir. 1985)	23
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978)	22

State Cases

<i>Commonwealth v. McCarthy</i> , 484 Mass. 493 (2020)	11
---	----

Federal Statutes

18 U.S.C. § 13	7
18 U.S.C. § 1151.....	7
18 U.S.C. § 1152	7
42 U.S.C. § 1983	21
47 O.S. § 10-102.1.....	7

Other Authority

Local Criminal Rule 16(A)	7
Google Privacy Policy, https://policies.google.com/privacy/archive/20190122	6, 15

**UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS
EVIDENCE OBTAINED BY GOOGLE "GEOFENCE" SEARCH WARRANT
AND BRIEF IN SUPPORT**

Comes now the United States of America, by Christopher J. Wilson, United States Attorney for the Eastern District of Oklahoma, and T. Cameron McEwen, Assistant United States Attorney, and respectfully requests this Court deny Defendant's Motion to Suppress Evidence Obtained by Google "*Geofence*" *Search Warrant* and Brief in Support (Doc. 39).

This issue is a matter of first impression for the Eastern District of Oklahoma and the Tenth Circuit. The Google geofence search warrant authorized location information associated with electronic devices that were within a geographical area approximately 1000' by 170', surrounding the scene of a fatal traffic collision between a vehicle and an individual on a bicycle. The geofence warrant also authorized location information for these devices for a period two minutes before and two minutes after the collision. This Court should deny Defendant's motion to suppress for three separate and independent reasons. First, the government did not conduct a search under the Fourth Amendment when it obtained this location information from Google. Second, the geofence warrant complied with the Fourth Amendment, as it was based on probable cause and specified its object with particularity. Third, suppression is inappropriate because investigators relied on the warrant in good faith.

I. BACKGROUND

On March 18, 2021, at 21:54 hours, a fatal traffic collision occurred at the intersection of U.S. Highway 62 and South 460 Road in Cherokee County, Oklahoma. This location is within the Eastern District of Oklahoma and within the definition of "Indian Country," as it occurred within the boundaries of the Cherokee Nation Indian Reservation.

Oklahoma Highway Patrol (“OHP”) troopers were dispatched to the scene. Based on OHP’s collection of evidence at the scene, including debris from a vehicle, and speaking to witnesses, investigators determined that a female, J.D., was travelling southbound on South 460 Rd. on her bicycle and was attempting to cross U.S. 62, when she was struck by an unknown vehicle travelling westbound on U.S. 62. J.D. was assisted by another motorist until she was transported by air ambulance to St. John Hospital in Tulsa, Oklahoma. J.D. later died from her injuries from the wreck. J.D. was confirmed as a member of the Cherokee Nation.

At the time of the collision, its location was a rural, four-lane highway separated by an unimproved median. There were no traffic control devices. There were a small number of commercial businesses and residences located near the intersection. OHP was able to retrieve surveillance video from several nearby businesses. A review of the videos shows that the collision occurred at 21:54 hours, and that shortly after the collision, the suspect vehicle pulled over to the shoulder of the highway a short distance from the collision. The suspect vehicle stopped for approximately 10 seconds before resuming westbound travelling on U.S. 62 and leaving the scene. In the one-minute timespan after the collision, the videos show six other vehicles travelling through the collision area. Five of the six vehicles are travelling eastbound.

On April 1, 2021, FBI Task Force Officer Dustin Thornton (“TFO Thornton”) sought and obtained a geofence search warrant. *See* Government’s Exhibits 1 and 2. Prior to applying for the geofence warrant, he discussed the matter with an assistant united states attorney with the Eastern District of Oklahoma. TFO Thornton’s affidavit for probable cause for the geofence warrant described the facts of the collision and evidence collected around the scene of the crime. *See* Government’s Exhibit 2 at pgs. 8-9. The affidavit also explained why there was reason to

believe that Google would have evidence pertaining to the collision. *Id.* at pages 3-10. Among other facts, the affidavit disclosed:

- (1) Google is a company that, among other things, offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device;
- (2) Google offers numerous apps and online-based services, including messaging and calling (e.g., Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (e.g., Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed into their Google accounts;
- (3) Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices;
- (4) Google offers accountholders a service called “Location History,” which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time;”
- (5) [T]he location information collected by Google and stored within an account’s Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device’s estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a ‘maps display radius,’ for each latitude and longitude point;
- (6) Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user’s location, to determine the user’s location when Google Maps is used, and to provide

location- based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months;

- (7) [A] vast majority of motorist not only own but use their smartphones while driving; and
- (8) [A] significant number of collisions occur as a result of distracted driving from a variety of sources, including cellphone use[,]” and “persons involved in a collision often use their cellphone immediately or shortly after a collision if not to call emergency services, then to call family members or friends.

Id. at pgs. 4-10. United States Magistrate Judge Steven P. Shreder of the Eastern District of Oklahoma issued the geofence warrant on a finding of probable cause. *See* Government’s Exhibit 2.

The geofence warrant specified a target geographical area, identified as an approximate 1000’ by 170’ area around specific latitude and longitude points surrounding the area of the collision. *See* Government’s Exhibit 2 at pg. 2. It authorized disclosure of location information for a period of two minutes before and two minutes after the collision from accounts associated with devices within this target area at some point during the four-minute interval that included the collision. *Id.* The geofence warrant also authorized disclosure of specified customer identity information associated with these accounts. *Id.* at pg. 3.

The geofence warrant authorized this disclosure through a three-step process that enabled law enforcement to “narrow down” the information disclosed by Google and thus obtain less than the maximum amount of information covered by the warrant. *Id.* The geofence warrant directed that in the first step, Google was to disclose information “specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available,” for “each location point recorded within the Initial Search Parameters, and for each location point recorded

outside the Initial Search Parameters where the margin of error (*i.e.*, “maps display radius”) would permit the device to be located within the Initial Search Parameters.” *Id.* In the second step, law enforcement was to review the anonymized location information produced by Google and identify the accounts of interest. *See id.* In the third step, law enforcement was to identify accounts that remained of interest, and Google was to disclose subscriber identity information for those accounts. *See id.*

Investigators followed this three-step process when they executed the geofence warrant. In step one, Google produced geolocation data in an anonymized format, which revealed three devices inside the “geofence” boundary. One of these devices crossed through the geofence from 21:54:18 to 21:54:35 with three location datapoints within the geofence. The timing and location of the datapoints of this device is consistent with the device travelling westbound on U.S. 62 at the exact moment of the collision and is consistent with the behavior of the suspect vehicle on video. In step two, investigators identified the accounts of interest, which was all three accounts, especially the account traveling westbound (“Suspect Account”). In step three, law enforcement requested and obtained subscriber information for at least two of the accounts, including the Suspect Account, which belonged to Defendant. This information revealed that the Google account associated with the device traveling westbound at the time of the collision is account XXXXXXXX6659. The name associated with the account is “sXXXXXX fXXXXXX” with an email of “XXXXXXXXXXXXX@gmail.com.” The account was created on March, 1, 2011, and uses a number of Google services and applications, including Web & App Activity, Gmail, Google Hangouts, iGoogle, Profiles, YouTube, Google Voice, Google Photos, Google Drive, Android, Google Calendar, Google Chrome Sync, Google Play Music, Google Docs, Google Play, Google

Takeout, Location History, Google Cloud Print, Blogger, Google My Maps, Is In Family, Google Payments, Google Keep, G1 Phone Backup, Play Loyalty, Device Centric Auth, Android Device Console, Has Google One Membership Information. Two cellphone numbers associated with the account are (XXX) XXX-1695 and (XXX) XXX-2760. The account was still active, with the most recent login (at the time the data was compiled in response to the search warrant) being April 11, 2021.

As the owner of a cellular phone that used a number of Google services and applications, Defendant affirmatively opted-in to Google's use and storage of her location information. *See* Google Privacy Policy (available at <https://policies.google.com/privacy/archive/20190122>) ("You can also turn on Location History if you want to create a private map of where you go with your signed-in devices."). She also had the ability to delete her location history. *See id.* In addition, she agreed to disclose her location information to Google for multiple purposes, including for Google to provide "personalized" services to her (including "content and ads" or "driving directions") and for Google to develop new services. *See id.*

On April 28, 2021, law enforcement obtained a search warrant signed by United States Magistrate Judge Kimberly E. West of the Eastern District of Oklahoma ordering Google to disclose additional location history data, before and after the collision, as well as any photos, messages, emails, queries, and other data held by Google pertaining to account 11352606659. *See* Government's Exhibits 3 and 4. The data returned by Google showed that one day after the crash, the user took a photo of a black Nissan Maxima, with damage to the front windshield, front passenger headlight, and front-end damage consistent with hitting a pedestrian. The vehicle also

was missing the tow hook cover found at the collision scene. Additionally, an examination of J.D.'s clothing found chips of black paint in her clothing.

Based on the Google location data revealed after the crash, the suspect vehicle drove to the Dallas-Fort Worth area and remained there for several days before traveling to Fayetteville, Arkansas. Based on a review of additional photos produced by Google, Defendant appeared to work at a construction site in Fayetteville with a large number of individuals. The data also revealed that after the collision the user searched Google for "taller mecanico near me," which translates to "mechanic workshop" or garage. There were also searches for "body shop," glass repair, and headlight replacement. Furthermore, using the location data, investigators were able to determine several locations that the user visited before and after the crash and followed up with those locations. These locations included the OYO motel in Irving, Texas and JR Body Shop in Dallas, Texas. Hotel staff confirmed that Defendant rented two rooms at the same motel.

As a result of the information and records obtained by law enforcement from Google along with other corroborating evidence linking Defendant to the suspect vehicle, Defendant was interviewed on October 20, 2021. In her interview, Defendant admitted to hitting a bicycle on her way from Arkansas to Dallas, Texas, but claimed she did not know someone was on it. She also admitted she was the sole occupant of the vehicle at the time of the collision.

On November 10, 2021, Defendant was charged in an Indictment by the Federal Grand Jury with one count of Failure to Stop for an Accident Involving Death in Indian Country, in violation of 18 U.S.C. § 13, 1151, and 1152 and 47 O.S. § 10-102.1. *See* Doc. 13.

On December 14, 2021, Defendant was arraigned on the Indictment and discovery was ordered pursuant to Local Criminal Rule 16(A). *See* Doc. 20. The United States produced

discovery materials to defense counsel on December 17, 2021, May 16, 2022, and October 13, 2022. This discovery included all requested documents and records obtained from Google LLC pursuant to the April 1, 2021 and April 28, 2021 search warrants.

On November 23, 2022, Defendant filed a Motion for Discovery Regarding Government's Use of Google's Sensorvault Data (Doc. 38) and this Opposed Motion to Suppress Evidence Obtained by *Google Geofence Search Warrant* and Brief in Support (Doc. 39).

II. ARGUMENT

A. Defendant Had No Reasonable Expectation of Privacy in the Four Minutes of Google Location Information

As set forth below, Defendant had no reasonable expectation of privacy in any of the information disclosed by Google pursuant to the geofence warrant. Defendant argues that she had a reasonable expectation of privacy in her location information under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), but *Carpenter* held only that the government infringes a cell phone owner's reasonable expectation of privacy when it accesses seven days or more of cell phone location information. *See Carpenter*, 138 S. Ct. at 2217 n.3. Here, the United States' acquisition of four minutes (two minutes before and after the collision) of Defendant's location information is governed by the long-standing principle that a person has no reasonable expectation of privacy in information disclosed to a third party and then conveyed by the third party to the government. It is important to note that Google also disclosed to the United States Defendant's basic subscriber information, including email address, Google Account ID, phone numbers associated with the account, and Google services used. In *United States v. Perrine*, the Tenth Circuit held that a subscriber has no reasonable expectation of privacy in such information. 518 F.3d 1196, 1204 (10th Cir. 2008); *see also United States v. Bynum*, 604 F.3d 161, 164 (4th

Cir. 2010) (holding that an internet and phone subscriber has no reasonable expectation of privacy). Defendant does not claim any protected privacy interest in this information.

1. Obtaining Four Minutes of Defendant's Location Information Was Not a Search Under *Carpenter*

Defendant's claims that based on *Carpenter* she had a reasonable expectation of privacy in the four minutes of location information disclosed by Google, but *Carpenter* does not bear the weight she places on it. In *Carpenter*, the Supreme Court determined that individuals have a "reasonable expectation of privacy in the whole of their physical movements," and it held "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." *Carpenter*, 138 S. Ct. at 2217 & n.3.

The Court emphasized that its decision was "a narrow one." *Carpenter*, 138 S. Ct. at 2220. It explicitly declined to determine whether there is a "limited period" for which the government can acquire cell phone location information without implicating the Fourth Amendment. *Id.* at 2217 n.3. It also explicitly refused to decide whether obtaining a cell tower dump constituted a Fourth Amendment search. *See id.* at 2220. This limitation is relevant here because tower dump information is similar to the information disclosed pursuant to the geofence warrant. A tower dump includes "information on all the devices that connected to a particular cell site during a particular interval." *Id.* Here, the geofence warrant sought information on all devices that were within a particular area during a particular interval.

Although *Carpenter* declined to resolve whether obtaining four minutes of cell phone location information constitutes a search, *Carpenter's* reasoning suggests it does not, because *Carpenter* is focused on protecting a privacy interest in long-term, comprehensive location information. The Court began its opinion by framing the question before it as "whether the

Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.” *Carpenter*, 138 S. Ct. at 2212. The Court emphasized that long-term cell-site information created a “comprehensive record of the person’s movements” that was “detailed” and “encyclopedic.” *Id.* at 2216–17. It explained that “this case is not about ‘using a phone’ or a person’s movement at a particular time. Rather, the Court explained, the case concerned a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years.” *Id.* at 2220. By this standard, the United States did not conduct a search when it obtained Defendant’s location information pursuant to the geofence warrant.

In addition, in numerous cases involving other sophisticated new technologies, lower courts held that *Carpenter* protects only comprehensive, long-term location information. For example, the Seventh Circuit recently held that real-time tracking of a specified cell phone over a period of approximately six hours was not a search. *See United States v. Hammond*, — F.3d —, 2021 WL 1608789 at *7-11 (7th Cir. Apr. 26, 2021). The Seventh Circuit previously determined that a cell tower dump was not a search, and two other district courts reached the same result. *See United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* “did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))” (emphasis in original)); *United States v. Walker*, 2020 WL 4065980 at *8 (W.D.N.C. July 20, 2020) (concluding that the “privacy concerns underpinning the court's holding in *Carpenter* do not come into play” for a cell tower dump, which is limited to “particular *place* at a *limited time*”) (emphasis in original)); *United State v. Rhodes*, 2021 WL 1541050 at *2 (N.D. Ga. Apr. 20, 2021) (stating that *Carpenter*

“centrally relied on the strong Fourth Amendment privacy interests implicated when law enforcement monitors or obtain voluminous, detailed cell phone information of a person's physical presence compiled over a lengthy period that effectively delineates the contours of the individual's life and communications”). These cases all support the conclusion that the United States did not infringe Defendant’s Fourth Amendment interests when it obtained four minutes of her location information from Google.

Similarly, courts have rejected a broad interpretation of *Carpenter* in cases involving automatic license plate reader databases, which record the time and place a license plate is observed. Obtaining a large amount of location information about an individual from such a database could potentially implicate *Carpenter*’s concerns regarding comprehensive location information. But investigators do not conduct a search when they obtain only a small quantity of location information from such a database. *See Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020) (“[W]hile the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of [automatic license plate readers], that interest is not invaded by the limited extent and use of ALPR data in this case.”); *United States v. Yang*, 958 F.3d 851, 862 (9th Cir. 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for Yang was not a search under *Carpenter* because “the information in the database did not reveal ‘the whole of [Yang’s] physical movements.’”).

Significantly, *Carpenter* did not reject the third-party doctrine or “disturb the application of *Smith* and *Miller*.” *Carpenter*, 138 S. Ct. at 2220 (citing *Smith v. Maryland*, 442 U.S. 735

(1979); *States v. Miller*, 425 U.S. 435 (1976)). Instead, *Carpenter* held that cell phone users do not voluntarily disclose their cell-site records to the phone company because cell-site information is collected “without any affirmative act on the part of the user beyond powering up,” because “there is no way to avoid leaving behind a trail of location data,” and because carrying a cell phone “is indispensable to participation in modern society.” *Carpenter*, 138 S. Ct. at 2220. These factors are not present here. Google could not obtain and store Defendant’s location without her undertaking multiple affirmative acts, including signing into Google on her phone, enabling the phone’s device location setting, enabling location reporting, and opting into Location History. Defendant also had discretion to delete any or all of her Location History. And none of the services associated with Google’s storage of Location History are indispensable to participation in modern society. Furthermore, *Carpenter*’s holding was based on facts specific to the cell phone provider context that *Carpenter* had not voluntarily disclosed his cell phone location information to the phone company, but it did not otherwise reverse or limit the third-party doctrine. *See Carpenter*, 138 S. Ct. at 2220. Thus, if this Court determines that Defendant intentionally disclosed her location to Google, this Court must conclude that Defendant had no reasonable expectation of privacy in the location information the United States obtained from Google, as “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. at 743-44.

Four Minutes of location data is only 1/2520th of the period that *Carpenter* held constituted a search, and it does not provide the sort of “all-encompassing record of the holder’s whereabouts” and “intimate window into a person’s life” that concerned the Court. *Carpenter*, 138 S. Ct. at 2217. Rather than providing an encyclopedic chronicle of Defendant’s life, the

information disclosed by Google provided a summary of her location for a short time period. This information is not quantitatively or qualitatively different from information that could be obtained from other sources, such as surveillance video or live witnesses.

Defendant's additional *Carpenter*-related arguments do not establish that the United States infringed his reasonable expectation of privacy. She argues that Google's information about its users' location is "more precise than the cell site location information at issue in *Carpenter*," Doc. 39 at pg. 10, but the Supreme Court in *Carpenter* stated that cell-site information "is rapidly approaching GPS-level precision," and *Carpenter*'s holding "[t]ook] account of more sophisticated systems that are already in use or in development." *Carpenter*, 138 S. Ct. at 2218-19. Thus, because the Supreme Court grounded *Carpenter*'s holding in an assumption that cell-site information would approach the precision of GPS, any distinction in precision between them cannot create enhanced Fourth Amendment protections for GPS information.

Defendant also argues that geofence information "Allows Law Enforcement to Retrospectively Locate Individuals in Time and Space," Doc. 39 at 11, but that fact does not distinguish geofence information from a wide variety of other business records, or even from witness testimony. For example, credit card records, landline telephone records, employee time sheets, and IP address records may enable law enforcement to retrospectively locate individuals at particular points in time. However, like the geofence information, none of these records provide a comprehensive inventory of the whole of a person's movements, and the United States does not infringe the privacy interest protected by *Carpenter* when it obtains them. *See, e.g., United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. June 13, 2019) (unpublished)

(holding that defendant had no reasonable expectation of privacy in IP address information, even after *Carpenter*).

2. Defendant Has No Reasonable Expectation of Privacy in Location Information She Disclosed to Google

Because *Carpenter* does not create a reasonable expectation of privacy in four minutes of location information, Google’s disclosure of that information to the United States is subject to the long-standing principle that an individual retains no reasonable expectation of privacy in information revealed to a third party and then disclosed by the third party to the United States. For decades, the Supreme Court has repeatedly invoked this third-party doctrine in cases ranging from private communications to business records, and this principle applies here to the defendant’s location information.

For example, in *Hoffa v. United States*, 385 U.S. 293 (1966), the Court applied the third-party doctrine to incriminating statements made in the presence of an informant. The Court held that the Fourth Amendment did not protect “a wrongdoer’s misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.” *Id.* at 302. A decade later the Supreme Court rejected a Fourth Amendment challenge to a subpoena for bank records in *United States v. Miller*, 425 U.S. 435 (1976). The Court held “that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.” *Id.* at 443; *see also SEC v. Jerry T. O’Brien, Inc.*, 467 U.S. 735, 743 (1984) (applying the third-party doctrine to financial records in the hands of a third-party).

The Supreme Court also relied on this principle in *Smith v. Maryland*, 442 U.S. 735 (1979), when it held that a telephone user had no reasonable expectation of privacy in dialed telephone number information. First, the Court stated that “we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.” *Id.* at 742. In addition, the Supreme Court further held that even if the defendant had a subjective expectation of privacy in his dialed telephone numbers, “this expectation is not one that society is prepared to recognize as reasonable.” *Id.* at 743 (internal quotation marks omitted). The Court explained that the user “voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business.” *Id.* at 743-44.

Defendant therefore had no reasonable expectation of privacy in Google’s records of her location because she voluntarily conveyed her location to Google in exchange for receiving the benefits of Google services. Because Google location service is an opt-in service, Defendant had previously taken an affirmative step to disclose her location information to Google. Moreover, she agreed that Google would have access to her location information for purposes ranging from providing him with targeted advertising or assistance with driving directions to Google’s development of new services. *See* Google Privacy Policy (available at <https://policies.google.com/privacy/archive/20190122>). These facts demonstrate that Defendant voluntarily disclosed her location information to Google, and the United States did not infringe on her reasonable expectation of privacy when it obtained from Google information her device’s location(s) during a four-minute interval.

The fact that Defendant voluntarily disclosed her location information to Google is confirmed by the reasoning of *Carpenter*. *Carpenter* concluded that cell-site information was not voluntarily disclosed to the phone company for two reasons, neither applicable here. First, the Court held that carrying a cell phone “is indispensable to participation in modern society.” *Carpenter*, 138 S. Ct. at 2220. In contrast, although Google services are frequently helpful and convenient, most may be used without turning on Google location services and using Google services with location enabled is not essential to participation in modern society. Google location services are no more indispensable than having a bank account or making a phone call, and bank records and dialed telephone number information remain unprotected by the Fourth Amendment under *Miller* and *Smith*. Second, *Carpenter* held that cell-site information is collected “without any affirmative act on the part of the user beyond powering up” and that “there is no way to avoid leaving behind a trail of location data.” *Id.* In contrast, in order for Google to have his location information, Defendant had to affirmatively opt in, and she also retained the ability to delete his information. Finally, a cell phone user’s disclosure of location information to the phone company is merely incidental to receiving communication service from the company, but a device owner’s disclosure of location information to Google is the central prerequisite to obtaining Google location services. Defendant thus voluntarily disclosed his location information to Google, and Google’s disclosure of that information to the United States did not infringe upon his reasonable expectation of privacy.

Finally, Defendant claims that obtaining her information from Google constitutes a search under “a property-based theory of the Fourth Amendment.” Doc. 39 at pg. 12. This argument is rooted in Justice Gorsuch’s solo dissent in *Carpenter*, where he discussed a transformation of

the Fourth Amendment that would jettison not only *Smith* and *Miller*, but also the reasonable expectation of privacy test of *Katz v. United States*, 389 U.S. 347 (1967). *See Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting). Ultimately, Justice Gorsuch concluded that *Carpenter* forfeited this new argument because he did not raise it below. *See id.* at 2272. Regardless, a solo dissent is not the law, and *Smith*, *Miller*, and *Katz* remain binding on this Court.

Under existing law, Google’s disclosure of location information to the United States did not infringe upon any reasonable expectation of privacy.

B. The Geofence Warrant Satisfied the Fourth Amendment

The geofence warrant did not remotely resemble a general warrant. A general warrant “specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.” *Steagald v. United States*, 451 U.S. 204, 220 (1981). In contrast, the geofence warrant authorized the United States to obtain from Google limited and specified information directly tied to a particular criminal offense at a particular place and time. As set forth below, because the warrant was supported by probable cause and specified its object with particularity, Defendant’s argument that the warrant was a general warrant is without merit. *See* Doc. 39 at pgs. 14-18.

More broadly, the facts of this case illustrate why a warrant that requires disclosure of information about devices in a particular place at a particular time is neither a general warrant nor, as Defendant asserts, “repugnant to the Constitution.” Doc. 39 at 14. When law enforcement officers sought the geofence warrant, they were investigating a serious crime, and

they had reason to believe that the perpetrator knowingly fled the scene after hitting someone on a bicycle. The geofence warrant allowed them to solve the crime and protect the public by examining a remarkably limited and focused set of records from Google: location information over a four-minute interval of Defendant and two other individuals. Rather than being “repugnant to the Constitution,” this investigative technique involved no unreasonable search or seizure and should be encouraged, not condemned.

1. The Geofence Affidavit Established Probable Cause

Probable cause requires only “a fair probability that contraband or evidence of a crime will be found in a particular place.” *United States v. Reed*, 195 Fed.Appx. 815, 821 (10th Cir. 2006) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (unpublished opinion); *see also United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019). It is “not a high bar.” *Bosyk*, 933 F.3d at 325 (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018). In addition, this Court does not conduct *de novo* review concerning the existence of probable cause: a “judge’s ‘decision to issue a warrant is entitled to great deference,’ and we ‘need only ask whether, under the totality of the circumstances presented in the affidavit, the ... judge had a ‘substantial basis’ for determining that probable cause existed.’” *Perrine*, 518 F.3d at 1201 (quoting *United States v. Artez*, 389 F.3d 1106, 1111 (10 Cir. 2004); *see also United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004) (quoting *Gates*, 462 U.S. at 238–39) (“the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.”).

Here, the affidavit in support of the warrant established an ample basis for the issuing magistrate judge’s finding of probable cause.

First, it established that an unknown subject was involved in a traffic collision with an individual on a bicycle at a particular place and time. *See* Government's Exhibit 1 at pgs. 8-9.

Second, "Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device." *Id.* at pgs. 4-5.

Third, "Google offers numerous apps and online-based services, including messaging and calling (e.g., Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (e.g., Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed into their Google accounts." *Id.* at 5.

Fourth, "Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices." *Id.*

Fifth, "Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time." *Id.* at pg. 6.

Sixth, "the location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending

on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a ‘maps display radius,’ for each latitude and longitude point.” *Id.*

Seventh, “Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user’s location, to determine the user’s location when Google Maps is used, and to provide location- based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months.” *Id.* at pgs. 6-7.

Eighth, “a vast majority of motorist not only own but use their smartphones while driving.” *Id.* at pg. 9.

Lastly, “a significant number of collisions occur as a result of distracted driving from a variety of sources, including cellphone use[,]” and “persons involved in a collision often use their cellphone immediately or shortly after a collision if not to call emergency services, then to call

family members or friends.” *Id.* at pg. 10. From this information, there was a substantial basis for the magistrate judge to find probable cause to believe that Google possessed evidence related to traffic collision.

The probable cause determination for a geofence warrant is similar to that for a tower dump warrant, and in *United States v. James*, No. 18-cr-216, 2019 WL 325231 (D. Minn. Jan. 25, 2019), the district court held that a series of tower dump warrants satisfied the Fourth Amendment. In *James*, the government used tower dump warrants to solve a series of robberies. The defendant there argued that there was no probable cause for the warrants because it was “unknown whether a phone was used by the suspect before or after the robbery.” *Id.* at *3. Nevertheless, the district court found that probable cause existed based on the affiant’s representations about the “ubiquitous nature” of cell phones, the likelihood of criminals using cell phones, and the storage by cell phone companies of location information. *Id.* This reasoning similarly supports the magistrate judge’s finding of probable cause for the geofence warrant in this case.

Messerschmidt v. Millender, 565 U.S. 535 (2012) demonstrates that the Supreme Court does not narrowly construe what may constitute evidence for purposes of a search warrant. In *Messerschmidt*, police obtained a warrant for “all guns and gang-related material” in connection with a known gang member shooting at his ex-girlfriend. *Id.* at 539. In a civil suit under 42 U.S.C. § 1983, Millender challenged the warrant as overbroad, but the Supreme Court rejected the suit based on qualified immunity. *See id.* The Court provided multiple reasons why it was not unreasonable for a warrant to seek “all gang-related materials” in connection with someone shooting at his ex-girlfriend. These reasons included that it could “help to establish motive,”

that it could be “helpful in impeaching [the shooter],” that it could be helpful in “rebutting various defenses,” and that it could “demonstrat[e] [the shooter’s] connection to other evidence.” *Id.* at 551-52.

Similarly, the issuing magistrate judge here had multiple reasons to believe that the location information for those present at the scene of the traffic collision would constitute evidence. Investigators could use the location information directly to reconstruct what took place at the crime scene at the time of the crime. They could use it to identify the suspect driver of the vehicle and those in the vehicle with the driver. They could use it to identify potential witnesses and obtain further evidence. They could use it to corroborate and explain other evidence, including surveillance video. They could use it to rebut potential defenses raised by the suspect driver, including an attempt by the suspect driver to blame someone else for her crime. Thus, although Defendant is correct that proximity to criminals does not alone give rise to probable cause that she committed a crime, *see* Doc. 39 at pg. 18, here probable cause existed for the location information sought by the warrant. The issuing magistrate judge had a substantial basis for finding probable cause to believe that Google possessed location information regarding the scene of the traffic collision, and this Court should therefore deny Defendant’s motion to suppress.

Finally, Defendant emphasizes that the geofence warrant collected information about persons not suspected of criminal activity, *see* Doc. 39 at pgs. 16-18, but this argument fails for several reasons and does not aid her Fourth Amendment argument. The Supreme Court has held that “it is untenable to conclude that property may not be searched unless its occupant is reasonably suspected of crime.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978). Instead,

a search warrant “may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises.” *Id.* Furthermore, the Supreme Court has squarely held that Fourth Amendment rights “may not be vicariously asserted.” *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Defendant therefore lacks standing to challenge the United States’ acquisition of others’ location information. *See, e.g., United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (rejecting defendant’s argument that investigator’s use of a cell-site simulator violated the privacy rights of third parties, because the defendant was “not entitled to invoke the rights of anyone else; suppression is proper only if the defendant’s own rights have been violated”). Additionally, these other individuals also voluntarily disclosed their location information to Google. Therefore, Google’s disclosure of other individuals’ location information pursuant to the geofence warrant did not infringe their Fourth Amendment rights either.

2. The Geofence Warrant Specified its Objects with Particularity

Under the Fourth Amendment, a valid warrant “must particularly describe the things to be seized, as well as the place to be searched.” *Dalia v. U.S.*, 441 U.S. 238, 239 (1979); *see also Mink v. Knox*, 613 F.3d 995, 1003 (10 Cir. 2010); *United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017). The “particularity requirement ensures that a search is confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause.” *U.S. v. Pulliam*, 748 F.3d 967 (10th Cir. 2014) (quoting *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985)). The particularity requirement also constrains a warrant so that it is “no broader than the probable cause on which it is based.” *United States v. Hurwitz*,

459 F.3d 463, 473 (4th Cir. 2006). Furthermore, “[t]he particularity requirement ‘ensures that the search will be carefully tailored to its justifications and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.’” *United States v. Otero*, 563 F.3d 1127, 1131-32 (10 Cir. 2009) (quoting *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)). In essence, it protects against “exploratory rummaging in a person's belongings.” *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (quoting *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)). Moreover, the test for particularity “is a pragmatic one” that “may necessarily vary according to the circumstances and type of items involved.” *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)).

Here, the geofence warrant was narrowly constrained based on location, dates, and times. The geofence warrant sought only location and identity information from Google regarding a four-minute interval for individuals present at the site of a traffic collision. Based on the facts and circumstances investigators knew about the collision, it was appropriately tailored toward its investigatory purpose, which was to obtain evidence to help identify the driver of a vehicle who struck an individual on a bicycle.

The cell tower dump opinion *James* provides persuasive authority that the warrant here was sufficiently particular. In *James*, the defendant argued that the tower dump warrants used to identify him as a robber were insufficiently particular because they “allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days during specific time frames.” *James*, 2019 WL 325231 at *3. The district court, however, found that the warrants were sufficiently particular because they sought information that was “constrained—both geographically and temporally—to the robberies under investigation.” *Id.*

This reasoning is fully applicable here: the geofence warrant was appropriately constrained in space and time to obtain evidence of the traffic collision. Indeed, the location information obtained from Google was more narrowly constrained than the location information in *James*. The target geographical area of 1000' by 170' identified in the GeoFence warrant is smaller than most cellular sites, and the United States only obtained location information regarding three individuals, rather than hundreds or thousands.

Defendant also challenges the geofence warrant because it included the three-step process for executing the warrant that “leaves the question of whose data to search and seize almost entirely [to] the discretion of the executing officers.” Doc. 39 at pg. 19-20. The geofence warrant, however, established probable cause for all the evidence that law enforcement could have obtained: identity information and four minutes of location data for all individuals present at or near the scene of the traffic collision. The information specified by a warrant must be “no broader than the probable cause on which it is based,” *Hurwitz*, 459 F.3d at 473, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. Rather than violating the Fourth Amendment, the three-step process allowed investigators to further protect privacy.

Finally, the most-heavily litigated search warrant in history—the search warrant in the investigation of the Playpen child pornography website—included a similar component that allowed investigators to prioritize the evidence they seized, and courts have agreed that that component did not violate the Fourth Amendment. Playpen was a dark web child pornography site with over 158,000 members. *See United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018). FBI investigators obtained a warrant authorizing a search of the computers of everyone

who logged into Playpen for 30 days. *See id.* at 689. The attached affidavit, however, allowed the FBI to choose to obtain less than the maximum amount of information the warrant authorized. It explained that that “in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users.” *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016). It is important to note that eleven Courts of Appeals have considered various challenges to the *Playpen* warrant, and all have ultimately rejected suppression. *See United States v. Taylor*, 935 F.3d 1279, 1281 (11th Cir. 2019) (“[W]e become today the eleventh (!) court of appeals to assess the constitutionality of the so-called ‘NIT warrant.’ Although the ten others haven’t all employed the same analysis, they’ve all reached the same conclusion—namely, that evidence discovered under the NIT warrant need not be suppressed.”); *see also United States v. Wagner*, 951 F. 3d 1232 (10th Cir. 2020); *United States v. Cookson*, 922 F.3d 1079 (10th Cir. 2019); *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017).

Some defendants argued that the discretion given the FBI in executing the *Playpen* warrant violated the Fourth Amendment’s particularity requirement, but courts uniformly rejected this argument. For example, in *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016), the court concluded that “the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site.” *See also Anzalone*, 208 F. Supp. 3d at 368 (“Every court to consider this question has found the NIT search warrant sufficiently particular.”). Similarly, the fact that investigators here could have and did narrow the information obtained from Google is immaterial, as the geofence warrant was based on probable cause and appropriately authorized seizure of location and identity information of anyone at the scene of the traffic collision. The

geofence warrant was not a general warrant, and this Court should deny Defendant's motion to suppress.

C. Evidence from the Geofence Warrant Should Not Be Suppressed Because Investigators Relied Upon It in Good Faith

Even assuming the geofence warrant was lacking in probable cause or particularity, suppression would not be an appropriate remedy. Suppression is a remedy of “last resort,” to be used for the “sole purpose” of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression “outweigh its heavy costs.” *Davis v. United States*, 564 U.S. 229, 236-37 (2011). “The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies.” *Herring v. United States*, 555 U.S. 135, 140 (2009). “To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Id.* at 144. Search warrants for Google information about the location of its users are a new and novel investigative technique. In *United States v. McLamb*, the Fourth Circuit rejected suppression in this circumstance. 880 F.3d 685 (4th Cir. 2018). The court held that when considering a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel and then sought a warrant:

But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what Leon's ‘good faith’ expects of law enforcement. We are disinclined to conclude that a warrant is ‘facially deficient’ where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

Id. at 691. Here, Task Force Officer Thornton followed the approach endorsed by *McLamb*. He

consulted with a federal prosecutor about the geofence warrant prior to obtaining it. In this investigation, he then sought and obtained a geofence search warrant from a United States magistrate judge. Thus, Task Force Officer Thornton did “precisely” what *McLamb* expects, and the good-faith exception precludes suppression here.

Alternatively, the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), leads to the same result: no suppression. When police act in “objectively reasonable reliance on a subsequently invalidated search warrant” obtained from a neutral magistrate, “the marginal or nonexistent benefits produced by suppressing evidence ... cannot justify the substantial costs of exclusion.” *Id.* at 922. *Leon* identified four circumstances in which an officer’s reliance on a warrant would not be objectively reasonable:

(1) when the issuing judge “was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth”; (2) when “the issuing magistrate wholly abandoned his judicial role ...”; (3) when “an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable”; or (4) when “a warrant [is] so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.”

United States v. Perez, 393 F.3d 457, 461 (4th Cir. 2004) (quoting *Leon*, 468 U.S. at 923). None of these circumstances are present in this case, and Defendant does not claim that the affiant misled the magistrate judge or that the magistrate judge abandoned his judicial role.

Defendant argues that the good faith exception does not apply here because a reasonable law enforcement officer could not have presumed that such an overbroad, unparticularized warrant would be valid, *see* Doc. 39 at pg. 21, but she is mistaken. As an initial matter, “the threshold for establishing this exception is a high one” because “[o]fficers executing warrants are not often expected to question the conclusions of an issuing authority.” *United States v.*

Seerden, 916 F.3d 360, 367 (4th Cir. 2019) (quoting *Messerschmidt*, 565 U.S. at 547); *see also Leon*, 468 U.S. at 898. Defendant asserts that “police knew they did not have a suspect, let alone probable cause to search any specific person or place. Instead, they sought every Google user’s location data along a strip of highway - with no evidence that the driver had ever used Google. They then exercised complete discretion in deciding which accounts to search further, deanonymize, and obtain additional information about. The deficiencies of this geofence warrant—its absence of probable cause and particularity—are readily apparent, casting it within the circumstances described in *Leon* and making the good faith exception to the exclusionary rule inapplicable.” Doc. 39 at pg. 21. However, Defendant ignores the fact that the affidavit established that the deceased individual was hit by a driver as she was crossing a roadway, the suspect driver likely had a cell phone in her possession at the time of the collision, and likely was either on the cell phone at the time of the collision or used it immediately after the collision to make an emergency call or call family or friends.

Neither the United States Supreme Court nor any of the Circuit Courts have addressed the issue of geofence warrants. However, one district court has recently addressed the matter. In *United States v. Chatrue*, 590 F.Supp.3d 901 (E.D. Virginia, Richmond Division 2022), the district court held that the geofence warrant violated the Fourth Amendment but denied the motion to suppress under the good faith exception. In *Chatrue*, the district court concluded that “[d]espite the warrant’s defects, the Court ultimately cannot find that excluding the instant evidence would serve to deter future improper law enforcement conduct. This is particularly so in light of rapidly advancing technology and lack of judicial guidance on this novel investigatory technique, and where, as here, prosecutors and magistrates approved three similar warrants.” *Id.*

at 936. The district court continued by stating, “evidence obtained pursuant to a search warrant issued by a neutral magistrate need not be excluded if the officer's reliance on the warrant was ‘objectively reasonable[,]’ and “[g]enerally, the fact that a neutral magistrate has issued a warrant ‘suffices to establish’ that a law enforcement officer has ‘acted in good faith in conducting the search.’” *Id.* at 937 (internal citations omitted). Furthermore, “consultation [with Government attorneys prior to seeking a warrant] is a relevant consideration in determining whether the warrant was facially deficient.” *Id.* (quoting *United States v. Matthews*, 12 F.4th 647, 657 (7th Cir. 2021)). Ultimately, the district court held that “[d]espite the warrant failing under Fourth Amendment scrutiny, the *Leon* good faith exception shields the resulting evidence from suppression.” *Chatrie*, 590 F.Supp.3d at 937. The district court also held that “[t]he warrant lacked particularized probable cause, but it was not ‘so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.’” *Id.* (quoting *Leon*, 468 U.S. at 923). The district court reasoned that “[t]his is particularly so because ‘the legality of [this] investigative technique [was] unclear,’ and [the officer] sought ‘advice from counsel before applying for the warrant.’” *Chatrie*, 590 F.Supp.3d at 937-38 (quoting *McLamb*, 880 F.3d at 691). This same rationale applies in this case. At the time TFO Thornton sought the geofence warrant, the legality of this investigative technique was unclear. In fact, it still is unclear. TFO Thornton also spoke with a federal prosecutor prior to applying for the search warrant. Therefore, based on the reasoning in *Chatrie* and TFO Thornton’s reasonable belief that the geofence warrant to Google was issued based on probable cause, the good faith exception precludes suppression.

III. CONCLUSION

Wherefore, the United States respectfully requests this Court deny Defendant's Motion to Suppress Evidence Obtained by Google "Geofence" Search Warrant and Brief in Support (Doc. 39).

CHRISTOPHER J. WILSON
United States Attorney

/s/ T. Cameron McEwen
T. CAMERON MCEWEN
AL BAR # 7161-R67M
Assistant United States Attorney
Eastern District of Oklahoma
520 Denison Ave.
Muskogee, OK 74401
(918) 684-5100
Cameron.McEwen@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on November 30, 2022, I electronically transmitted the attached documents to the Clerk of Court using the ECF System for filing. Based on the records currently on file, the Clerk of Court will transmit a Notice of Electronic Filing to the following ECF registrants:

Juan L. Guerra, Jr., Attorney for Defendant

/s/ T. Cameron McEwen
T. CAMERON MCEWEN
Office of the United States Attorney